tion (1.3.3) starting with only a finite number of them. In group-theoretical language, the following result is true.

Theorem 1.3 (Mordell's Theorem). *The Abelian group $\mathcal{C}(\mathbb{Q})$ is finitely generated.*

(cf. ([Mor22], [Cas66], [Mor69], [La83], [Se97] and Appendix by Yu.Manin to [Mum74]). From the structure theorem for finitely generated Abelian groups, it follows that

$$\mathcal{C}(\mathbb{Q}) \cong \Delta \times \mathbb{Z}^r$$

where Δ is a finite subgroup consisting of all torsion points, and $\mathbb{Z}^r$ is a product of r copies of an infinite cyclic group. The number r is called *the rank* of $\mathcal{C}$ over $\mathbb{Q}$.

The group Δ can be found effectively. For example, Nagell and Lutz (cf. [Lu37]) proved that torsion points on a curve $y^2 = x^3 + ax + b$ for which a and b are integers, have integral coordinates. Furthermore, the y–coordinate of a torsion point either vanishes or divides $D = -4a^3 - 27b^2$.

B.Mazur proved in 1976 that the torsion subgroup Δ over $\mathbb{Q}$ can only be isomorphic to one of the following fifteen groups:

$$\mathbb{Z}/m\mathbb{Z}\ (m \leq 10, m = 12),\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}\ (n \leq 4), \tag{1.3.7}$$

and all these groups occur, cf. [Maz77].

It is still an open question whether r can be arbitrarily large. Mestre (cf. [Me82]) constructed examples of curves whose ranks are at least 14. *)

A comparatively simple example of a curve of rank ≥ 9 is also given there: $y^2 + 9767y = x^3 + 3576x^2 + 425x - 2412$. One can conjecture that rank is unbounded. B. Mazur (cf. [Maz86]) connects this conjecture with *Silverman's conjecture* (cf. [Silv86]) that for any natural k there exists a cube-free integer which can be expressed as a sum of two cubes in more than k ways.

Examples. 1) Let $\mathcal{C}$ be given by the equation

$$y^2 + y = x^3 - x$$

whose integer solutions list all cases when a product of two consecutive integers equals a product of three consecutive integers. Here Δ is trivial while the free part of $\mathcal{C}(\mathbb{Q})$ is cyclic, with a generator $P = (0, 0)$. Points mP (labeled by m) are shown in Figure 9.

The following Table 1.3, reproduced here from [Maz86] with Mazur's kind permission, shows the absolute values of the X–coordinates of points mP, for even m between 8 and 58.

* Martin–Mcmillen (2000) found an elliptic curve of rank ≥ 24:

$$\begin{aligned} y^2 + xy + y = x^3 &- 120039822036992245303534619191166796374x \\ &+ 504224992484910670010801799168082726759443756222911415116 \end{aligned}$$

(see http://www.math.hr/~duje/tors/rankhist.html for more examples). (footnote by Yu.Tschinkel).

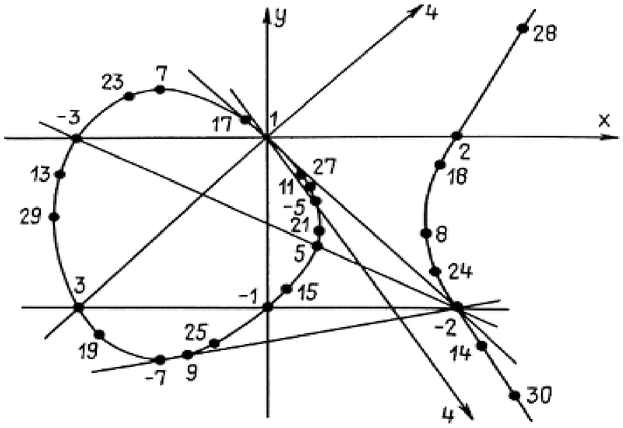

Fig. 1.9.

Table 1.3.

20
116
3741
8385
239785
59997896
18490337896
270896443865
16683000076735
2786836257692691
314892968128574 0316
34211575692760792 7420
2802511299225632914 22645
804287518035141565236193151
74304313429704905352925 2783151
3239336802390544740129153150480400
261339025245801434436942401261367 9600
1251873709467123982668303194358315 2550351
596929565407758846078157850477988229836340351
23858585863298296316080775539381392644313520 10155
561860540184347535270227523822802918820488095828573 80
23897505191109140186309909376606354352699564527703566 25916
650087890787664552756007507113064937939959207504295469122 18291
863381503588680671392136126345657274078403806591767431591377 5417535
4327678343894888631258803040444144431340575553436625441643288092 4019065
593076045469642658948956761739794324482729234687114512318727773285587 6671389

One sees that the last figures lie approximately on a parabola. This is not an accident, but a reflection of the *quadratic nature of heights on elliptic curves* (cf. below).

2) Table 1.4 was kindly calculated for this edition by H.Cohen, using PARI computing system, [BBBCO]. This table lists ranks r and generators for curves $X^3 + Y^3 = AZ^3$ with natural cube-free $A \leq 500$; it corrects and completes the Tables of Selmer (cf. [Selm51], [Selm54]) which were reproduced in the first edition [Ma-Pa]. Note the 3 missing values $A = 346, 382, 445$ for which H.Cohen proved that $r = 1$, but the method of Heegner points for computing